METHOD, SYSTEM AND APPARATUS ENCRYPTING, APPARATUS FOR DECRYPTING AND COMPUTER PROGRAM

Patent Number: JP2003005645
Publication date: 2003-01-08
Inventor(s): KAMEDA TOSHITADA; IWAI TSUTOMU
Applicant(s): KAMEDA TOSHITADA
Requested Patent: ☐ JP2003005645
Application Number: JP20010184758 20010619
Priority Number(s):
IPC Classification: G09C1/00; G06F12/14
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To protect individual privacy associated with personal data of patients, etc., treated in facilities associated with medical care and allow processing analysis and statistics of the data of the patients, etc.
SOLUTION: An encrypting method includes a selecting process for selecting a field corresponding to an item capable of identifying an individual in a personal data file including personal records comprising a plurality of the fields having the personal data encoded, digitized and converted into text in unified format item by item, a partially encrypting process for encrypting the selected field by using the first public key, not encrypting unselected fields and producing a partially encrypted file, a wholly encrypting process for encrypting the partially encrypted file and producing a wholly encrypted file and a wholly decrypting process for decrypting the produced wholly encrypted file and reproducing the partially encrypted file.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2003－5645
（P2003－5645A）
(43)公開日　平成15年1月8日(2003.1.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｊ１０４

審査請求　有　　請求項の数20　ＯＬ　（全 19 頁）

(21)出願番号　特願2001－184758(P2001－184758)

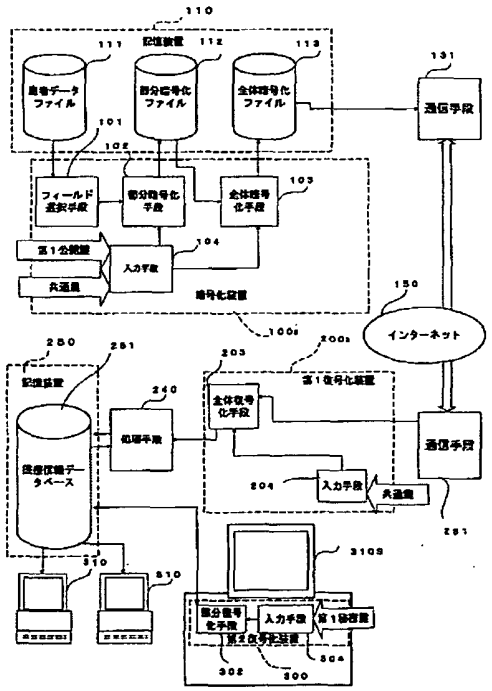
(22)出願日　平成13年６月19日(2001.6.19)

(71)出願人　599115734
亀田　俊忠
千葉県鴨川市東町929
(72)発明者　亀田　俊忠
千葉県鴨川市東町929
(72)発明者　岩井　勉
東京都港区虎ノ門３丁目18番16号菅井ビル６階　株式会社亀田医療情報研究所内
(74)代理人　100104765
弁理士　江上　達夫

Ｆターム(参考)　5B017 AA07 BA07 CA16
5J104 AA16 EA06 EA19 NA02 PA07

(54)【発明の名称】　暗号方法、暗号システム、暗号化装置、復号化装置及びコンピュータプログラム

(57)【要約】
【課題】　医療関連施設等で扱われる患者データ等の個人データに係る個人のプライバシーを守りながら、患者データ等の解析処理や統計処理を行えるようにする。
【解決手段】　暗号方法は、個人データを統一フォーマットで項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる個人レコードを含んでなる個人データファイルの中で、個人を特定可能とされる項目に対応するフィールドを選択する選択工程と、該選択されたフィールドを第１公開鍵で暗号化すると共に選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化工程と、この部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化工程とを含む。更に、このように作成された全体暗号化ファイルを復号化して部分暗号化ファイルを再生する全体復号化工程を含む。



【特許請求の範囲】

【請求項１】 所定単位の個人データを統一フォーマットで項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる個人レコードを少なくとも一つ含んでなる個人データファイルの中で、所定基準に従って個人を特定可能とされる項目に対応するフィールドを選択する選択工程と、該選択されたフィールドを第１公開鍵で暗号化すると共に前記選択工程により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化工程と、

該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化工程と、該作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化工程とを備えたことを特徴とする暗号方法。

【請求項２】 前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第１公開鍵に対応する第１秘密鍵で復号化して前記個人データファイルを再生する部分復号化工程を更に備えたことを特徴とする請求項１に記載の暗号方法。

【請求項３】 前記選択工程は、前記所定基準として段階的な複数の基準に従って前記フィールドを段階的に選択し、前記部分暗号化工程は、前記段階的に選択されたフィールドを、段階毎に異なる第１公開鍵で暗号化することを特徴とする請求項１に記載の暗号方法。

【請求項４】 前記全体復号化工程により再生された部分暗号化ファイルのうち前記段階的に選択されたフィールドを前記段階毎に異なる第１公開鍵に対応する第１秘密鍵で復号化する部分復号化工程を更に備えたことを特徴とする請求項３に記載の暗号方法。

【請求項５】 前記全体暗号化工程は、共通鍵で前記部分暗号化ファイルを暗号化する工程と、該共通鍵を第２公開鍵で暗号化する工程とを含み、前記全体復号化工程は、前記第２公開鍵に対応する第２秘密鍵で前記共通鍵を復号化する工程と、該復号化された共通鍵で前記全体暗号化ファイルを復号する工程とを含むことを特徴とする請求項１から４のいずれか一項に記載の暗号方法。

【請求項６】 前記全体暗号化工程は、第２公開鍵で前記部分暗号化ファイルを暗号化し、

前記全体復号化工程は、前記第２公開鍵に対応する第２秘密鍵で前記全体暗号化ファイルを復号化することを特徴とする請求項１から４のいずれか一項に記載の暗号方法。

【請求項７】 前記部分暗号化ファイルに対し、前記個人レコード毎に個人ＩＤコードとは異なるレコード識別子を付与する工程を更に含み、

前記部分暗号化工程は、前記レコード識別子に基づいて前記個人レコードの統計処理又は解析処理が可能なように、前記選択されたフィールドを暗号化することを特徴とする請求項１から６のいずれか一項に記載の暗号方法。

【請求項８】 所定単位の個人データを統一フォーマットで項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる個人レコードを少なくとも一つ含んでなる個人データファイルの中で、所定基準に従って個人を特定可能とされる項目に対応するフィールドを選択する選択手段と、該選択されたフィールドを第１公開鍵で暗号化すると共に前記選択手段により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化手段と、

該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化手段と、該作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化手段とを備えたことを特徴とする暗号システム。

【請求項９】 前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第１公開鍵に対応する第１秘密鍵で復号化して前記個人データファイルを再生する部分復号化手段を更に備えたことを特徴とする請求項８に記載の暗号システム。

【請求項１０】 前記選択手段は、前記所定基準として段階的な複数の基準に従って前記フィールドを段階的に選択し、

前記部分暗号化手段は、前記段階的に選択されたフィールドを、段階毎に異なる第１公開鍵で暗号化することを特徴とする請求項８に記載の暗号システム。

【請求項１１】 前記全体復号化手段により再生された部分暗号化ファイルのうち前記段階的に選択されたフィールドを前記段階毎に異なる第１公開鍵に対応する第１秘密鍵で復号化する部分復号化手段を更に備えたことを特徴とする請求項１０に記載の暗号システム。

【請求項１２】 前記全体暗号化手段は、共通鍵で前記部分暗号化ファイルを暗号化する手段と、該共通鍵を第２公開鍵で暗号化する手段とを含み、前記全体復号化手段は、前記第２公開鍵に対応する第２秘密鍵で前記共通鍵を復号化する手段と、該復号化された共通鍵で前記全体暗号化ファイルを復号する手段とを含むことを特徴とする請求項８から１１のいずれか一項に記載の暗号システム。

【請求項１３】 前記全体暗号化手段は、第２公開鍵で前記部分暗号化ファイルを暗号化し、

前記全体復号化手段は、前記第２公開鍵に対応する第２秘密鍵で前記全体暗号化ファイルを復号化することを特徴とする請求項８から１１のいずれか一項に記載の暗号システム。

【請求項１４】 前記部分暗号化ファイルに対し、前記個人レコード毎に個人ＩＤコードとは異なるレコード識別子を付与する手段を更に含み、

前記部分暗号化手段は、前記レコード識別子に基づいて前記個人レコードの統計処理又は解析処理が可能なよう

に、前記選択されたフィールドを暗号化することを特徴とする請求項8から13のいずれか一項に記載の暗号システム。

【請求項15】 所定単位の個人データを統一フォーマットで項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる個人レコードを少なくとも一つ含んでなる個人データファイルの中で、所定基準に従って個人を特定可能とされる項目に対応するフィールドを選択する選択手段と、該選択されたフィールドを第1公開鍵で暗号化すると共に前記選択手段により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化手段と、該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化手段とを備えた暗号化装置。

【請求項16】 請求項15に記載の暗号化装置により作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化手段を備えたことを特徴とする復号化装置。

【請求項17】 前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第1公開鍵に対応する第1秘密鍵で復号化して前記個人データファイルを再生する部分復号化手段を更に備えたことを特徴とする請求項16に記載の復号化装置。

【請求項18】 コンピュータを請求項8から14のいずれか一項に記載の暗号システムとして機能させることを特徴とするコンピュータプログラム。

【請求項19】 コンピュータを請求項15に記載の暗号化装置として機能させることを特徴とするコンピュータプログラム。

【請求項20】 コンピュータを請求項16又は17に記載の復号化装置として機能させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、例えば医療関連施設で扱われる患者データ等の個人データに係る個人のプライバシーを保護するために用いられる暗号方法、暗号システム、暗号化装置、復号化装置及びコンピュータプログラムの技術分野に属する。

【0002】

【従来の技術】この種の暗合方法には、一般に共通鍵暗号方式、秘密鍵暗号方式、公開鍵暗号方式による暗号方法がある。

【0003】共通鍵暗号方式とは、1個の共通鍵で暗号化した場合には、暗号化されたデータを、同じ共通鍵を使って復号化する方式である。

【0004】秘密鍵暗号方法とは、どのような方法で暗号化するかというアルゴリズムを不特定多数人で利用可能なように公開する一方で、暗号化する鍵及び復号化する鍵を秘密にしておき、これらの秘密の鍵を用いて暗号化及び復号化する方式である。この場合、暗号化の鍵と復号化の鍵とを同じにするのが普通であり、一般に上述の共通鍵暗号方式と同義で扱われることが多い。尚、このような秘密鍵或いは共通鍵は、暗号化本来の目的のためには、発信者と受信者が夫々第3者に知られないように保管することが前提となる。

【0005】他方、公開鍵暗号方式とは、暗号化する鍵である公開鍵でデータを暗号化した場合には、暗号化されたデータを、これとは異なる復号化の鍵であると共に秘密である（即ち、発信者には知られない）秘密鍵で復号化する方式である。

【0006】これらの各種暗号方法を、例えば特開平2000−331101号公報、特開平11−102317号公報、特開平11−053668号公報等に開示されているように医療関連施設で用いれば、暗号化された患者データ等の個人データを通信手段を介して転送或いは移送する途中で、データが漏洩しても或いは盗まれても、共通鍵や秘密鍵がない限り、データを複合化できないので、個人データに係るプライバシーを保護できるとされている。

【0007】

【発明が解決しようとする課題】しかしながら、上述した各種暗号方法によれば、暗号前にデータを取り扱う、例えば病院等の医療関連施設では、守秘義務がある医師、看護婦、検査技師、薬剤師等しか患者データ等を見ることはできないものの、患者データ等の復号化後にデータを扱う、例えば研究施設、公的機関、他の病院、大学等の他の医療関連施設では、一般に守秘義務のない研究員、調査員、事務員等であっても患者データ等を見ることが可能になる。そして、例えば患者データ上で患者の氏名に係る項目を伏せておいたとしても、故意又は偶然により患者データに係る患者個人が、例えば性別、生年月日、入院年月日、退院年月日、病歴、通院暦等の項目など、患者データのいずれかの項目から特定されてしまう可能性が高いという大きな問題点がある。即ち、暗号化した患者データ等に対しては、復号化後に、医療関係の各種統計処理や解析処理が行われる性質上、各種関係者の目に触れる状態となるため、患者データ等の個人データに係るプライバシーの保護を図ることが実際上は極めて困難となる。この際特に、例えば患者が特定されるのを完全に避けた形では、患者データを医療向上のための解析に利用することは困難であり、逆に、例えば医療向上のために各種患者データを利用可能とすれば、氏名を伏せておく程度では、性別、生年月日、入院年月日、退院年月日、病歴、通院暦等を通じて患者が特定されてしまうという解決困難な問題点がある。

【0008】本発明は上述の問題点に鑑みなされたものであり、患者等の個人のプライバシーを守りながら、患者データ等の個人データの解析処理や統計処理を可能ならしめる暗号方法、暗号システム、暗号化装置、復号化装

置、並びにコンピュータをそのような暗号システム、暗号化装置及び復号化装置として機能ならしめるコンピュータプログラムを提供することを課題とする。

【０００９】

【課題を解決するための手段】本発明の暗号方法は上記課題を解決するために、所定単位の、例えば患者データ等の個人データを統一フォーマットで、例えば医療関連項目等の項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる、例えば患者レコード等の個人レコードを少なくとも一つ含んでなる、例えば患者データファイル等の個人データファイルの中で、所定基準に従って、例えば患者個人等の個人を特定可能とされる項目に対応するフィールドを選択する選択工程と、該選択されたフィールドを第１公開鍵で暗号化すると共に前記選択工程により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化工程と、該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化工程と、該作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化工程とを備える。

【００１０】本発明の暗号方法によれば、先ず選択工程により、複数フィールドからなる患者レコード等の個人レコードを含んでなる患者データファイル等の個人データファイルの中で、所定基準に従って、患者個人等の個人を特定可能とされる項目に対応するフィールドを選択する。ここに「個人レコード」とは、例えば患者レコードを例にとれば、１入院単位、１レセプト単位、１カルテ単位等の患者データを取り扱う上でまとめられた記録の単位であるが、より一般には何らかの個人データを取り扱う上でまとめられた記録の単位である。この選択工程では、例えば患者ＩＤに対応するフィールド、患者の生年月日に対応するフィールド、退院年月日に対応するフィールド、入院年月日に対応するフィールドなど、患者を特定可能とされる項目等に対応するフィールドを選択するが、より一般には個人を特定可能とされる項目に対応するフィールドを選択する。このような患者個人等の個人を特定可能か否かについての所定基準は、経験的、実験的、理論的に予め設定しておけばよく、実際の使用環境に応じて個別具体的に変更を加えてもよい。そして、部分暗号化工程により、このように選択されたフィールドを第１公開鍵で暗号化すると共に選択されないフィールドを暗号化しないことにより、部分暗号化ファイルを作成する。続いて、全体暗号化工程により、この作成された部分暗号化ファイルを、例えば共通鍵方式、秘密鍵方式、公開鍵方式等の公知の暗号化方式で暗号化して、全体暗号化ファイルを作成する。その後、この全体暗号化ファイルが、インターネット等の通信手段を通じて、例えば病院等の一の医療関連施設から医療研究所などの他の医療関連施設に転送されたり、フレキシブルディスク、ＣＤ−ＲＡＭ等の記憶媒体に格納された状態で移送される。この際、当該全体暗号化ファイルが漏洩したり盗難されたりしても、全体が暗号化されているので、意味が理解されることは無い。その後、転送或いは移送先である、例えば他の医療関連施設等で、全体復号化工程により、この全体暗号化ファイルを復号化して部分暗号化ファイルを再生する。しかるに本発明によれば、このように他の医療関連施設等で再生された部分暗号化ファイルにおいては、個人を特定可能とされるフィールドが、未だ第１公開鍵で暗号化された状態にあるので、例えば研究施設、公的機関、他の病院、大学等の当該他の医療関連施設で一般に守秘義務のない研究員、調査員、事務員等がこのような部分暗号化ファイルの一部として、患者データ等の個人データを見ても、これに係る個人が特定されてしまう可能性が顕著に低減される。即ち、個人データの転送や移送後における、例えば医療関係等の各種統計処理や解析処理の際に、例えば病名、術式、治療結果、治療薬等の個人データが各種関係者の目に触れる状態となっても、個人が特定されないので、各個人におけるプライバシーの保護を図ることができる。この際特に、個人を特定可能とされる項目についての基準を調節すれば、個人が特定されることを避けつつ、例えば患者データを各種解析や統計処理に利用することが可能となる。例えば、患者データ上で氏名、性別、生年月日、入退院年月日、病歴、通院暦等に対応するフィールドについては、意味が理解されないように、前記所定基準を予め設定しておけば、部分暗号化ファイルを見ても患者が特定されてしまう可能性は殆ど或いは実践的な意味で全くなくなる。逆に、暗号化されていないフィールドを見れば、例えば、この患者は、今までに何回入院したのか？以前に入院したのか？以前にどのような治療をしたのか？などの情報を、個人を特定することなく分析でき、例えば症例分析、病院評価、術式評価、投薬評価等の各種の統計処理や解析処理を行える。

【００１１】以上のように、本発明の暗号方法によれば、個人のプライバシーを守りながら、個人データの解析処理や統計処理を行うことが可能となる。

【００１２】本発明の暗号方法の一態様では、前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第１公開鍵に対応する第１秘密鍵で復号化して前記患者データファイルを再生する部分復号化工程を更に備える。

【００１３】この態様によれば、部分復号化工程により、再生された部分暗号化ファイルのうち、未だ暗号化されているフィールドを、第１公開鍵に対応する第１秘密鍵で復号化して、例えば患者データファイル等の個人データファイルを再生する。従って、当該個人データについて守秘義務のある、例えば主治医等の特定人のみに第１秘密鍵を知らせておけば、この者のみが復号化後の個人データの全てを見ることができる。

【００１４】或いは本発明の暗号方法の他の態様では、

前記選択工程は、前記所定基準として段階的な複数の基準に従って前記フィールドを段階的に選択し、前記部分暗号化工程は、前記段階的に選択されたフィールドを、段階毎に異なる第１公開鍵で暗号化する。

【００１５】この態様によれば、個人を特定可能とされる所定基準を段階分けする。例えば、個人を特定するのが非常に容易な、氏名、住所、患者ＩＤなどについては第１基準とし、生年月日、入院月日、退院月日等については第２基準とし、入院期間、病歴、慢性病歴等については第３基準とし、これらに従って、フィールドを段階毎に異なる第１公開鍵で暗号化する。従って、個人の特定のし易さに応じて別々の暗号化の鍵で暗号化でき、最終的には、別々の復号化の鍵で復号化できる。

【００１６】この態様では、前記全体復号化工程により再生された部分暗号化ファイルのうち前記段階的に選択されたフィールドを前記段階毎に異なる第１公開鍵に対応する第１秘密鍵で復号化する部分復号化工程を更に備えてもよい。

【００１７】このように構成すれば、復号化後の部分暗号化ファイルを、例えば所長、副所長、事務委員長、研究者、事務員等の立場が異なる人間に対して異なる秘密鍵を知らせることにより、その立場に応じて見ることができる、患者データ等の個人データの種類を変えられる。このため、個人のプライバシーを保護しつつ立場に応じて必要な個人データを提供でき、大変便利である。

【００１８】本発明の暗号方法の他の態様では、前記全体暗号化工程は、共通鍵で前記部分暗号化ファイルを暗号化する工程と、該共通鍵を第２公開鍵で暗号化する工程とを含み、前記全体復号化工程は、前記第２公開鍵に対応する第２秘密鍵で前記共通鍵を復号化する工程と、該復号化された共通鍵で前記全体暗号化ファイルを復号する工程とを含む。

【００１９】この態様によれば、全体暗号化工程により、全体暗号化ファイルは、暗号化された公開鍵たる第２公開鍵で暗号化されていることとなり、当該全体暗号化ファイルの転送時や移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００２０】或いは本発明の暗号方法の他の態様では、前記全体暗号化工程は、第２公開鍵で前記部分暗号化ファイルを暗号化し、前記全体復号化工程は、前記第２公開鍵に対応する第２秘密鍵で前記全体暗号化ファイルを復号化する。

【００２１】この態様によれば、全体暗号化ファイルは、第２秘密鍵がなければ復号化できないので、当該全体暗号化ファイルの転送時や移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００２２】本発明の暗号方法の他の態様では、前記部分暗号化ファイルに対し、前記個人レコード毎に個人ＩＤコードとは異なるレコード識別子を付与する工程を更に含み、前記部分暗号化工程は、前記レコード識別子に基づいて前記個人レコードの統計処理又は解析処理が可能なように前記選択されたフィールドを暗号化する。

【００２３】この態様によれば、個人のプライバシーを保護したまま、部分暗号化ファイルを、例えば患者ＩＤではなく、入院単位等の患者レコード毎に付与されたレコード識別子に基づいて、統計処理又は解析処理が可能となり、医療情報データベース等のデータベースを構築することも可能となる。例えば、同じコードは同じコードに変換し、同じデジタル値は同じデジタル値に変換し、或いは同じテキストは同じテキストに変換する可逆方式の暗号化方式により、各フィールドを選択的に暗号化することで、暗号化された状態（即ち個人を特定できない状態）のままで、例えば病院評価、症例分析、術式評価、投薬評価等の統計処理や解析処理を行える。しかも、守秘義務のある関係機関や関係者によって、フィールドを部分的に暗号化した際に用いた第１公開鍵に対応する第１秘密鍵を用いて部分復号化処理を行えば、このように統計処理や解析処理の結果上における個人データを全て見ることも可能となる。

【００２４】本発明の暗号システムは上記課題を解決するために、所定単位の、例えば患者データ等の個人データを統一フォーマットで、例えば医療関連項目等の項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる、例えば患者レコード等の個人レコードを少なくとも一つ含んでなる、例えば患者データファイル等の個人データファイルの中で、所定基準に従って、例えば患者個人等の個人を特定可能とされる項目に対応するフィールドを選択する選択手段と、該選択されたフィールドを第１公開鍵で暗号化すると共に前記選択手段により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化手段と、該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化手段と、該作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化手段とを備える。

【００２５】本発明の暗号システムによれば、先ず選択手段により、複数フィールドからなる個人レコードを含んでなる個人データファイルの中で、所定基準に従って、個人を特定可能とされる項目に対応するフィールドを選択する。そして、部分暗号化手段により、このように選択されたフィールドを第１公開鍵で暗号化すると共に選択されないフィールドを暗号化しないことにより、部分暗号化ファイルを作成する。続いて、全体暗号化手段により、この作成された部分暗号化ファイルを暗号化して、全体暗号化ファイルを作成する。その後、この全体暗号化ファイルが、インターネット等の通信手段を通じて転送されたり、記憶媒体に格納された状態で移送される。この際、当該全体暗号化ファイルが漏洩したり盗難されたりしても、全体が暗号化されているので、意味が理解されることは無い。その後、転送或いは移送先であ

る、例えば他の医療関連施設等で、全体復号化手段により、この全体暗号化ファイルを復号化して部分暗号化ファイルを再生する。

【００２６】従って本発明の暗号システムによれば、上述した本発明の暗号方法の場合と同様に、個人のプライバシーを守りながら、個人データの解析処理や統計処理を行うことが可能となり、最終的には個人データを医療等の各種産業で有効利用できる。

【００２７】本発明の暗号システムの一態様では、前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第１公開鍵に対応する第１秘密鍵で復号化して前記患者データファイルを再生する部分復号化手段を更に備える。

【００２８】この態様によれば、部分復号化手段により、再生された部分暗号化ファイルのうち、未だ暗号化されているフィールドを、第１公開鍵に対応する第１秘密鍵で復号化して、個人データファイルを再生する。従って、当該個人データについて守秘義務のある特定人のみに第１秘密鍵を知らせておけば、この者のみが復号化後の個人データの全てを見ることができる。

【００２９】或いは本発明の暗号システムの他の態様では、前記選択手段は、前記所定基準として段階的な複数の基準に従って前記フィールドを段階的に選択し、前記部分暗号化手段は、前記段階的に選択されたフィールドを、段階毎に異なる第１公開鍵で暗号化する。

【００３０】この態様によれば、個人を特定可能とされる所定基準を段階分けし、これらに従って、フィールドを段階毎に異なる第１公開鍵で暗号化する。従って、個人の特定のし易さに応じて別々の暗号化の鍵で暗号化でき、最終的には、別々の復号化の鍵で復号化できる。

【００３１】この態様では、前記全体復号化手段により再生された部分暗号化ファイルのうち前記段階的に選択されたフィールドを前記段階毎に異なる第１公開鍵に対応する第１秘密鍵で復号化する部分復号化手段を更に備えてもよい。

【００３２】このように構成すれば、復号化後の部分暗号化ファイルを、立場が異なる人間に対して異なる秘密鍵を知らせることにより、その立場に応じて見ることができる個人データの種類を変えられる。このため、個人のプライバシーを保護しつつ立場に応じて必要な個人データを提供でき、大変便利である。

【００３３】本発明の暗号システムの他の態様では、前記全体暗号化手段は、共通鍵で前記部分暗号化ファイルを暗号化する手段と、該共通鍵を第２公開鍵で暗号化する手段とを含み、前記全体復号化手段は、前記第２公開鍵に対応する第２秘密鍵で前記共通鍵を復号化する手段と、該復号化された共通鍵で前記全体暗号化ファイルを復号する手段とを含む。

【００３４】この態様によれば、全体暗号化手段により、全体暗号化ファイルは、暗号化された公開鍵たる第２公開鍵で暗号化されていることとなり、当該全体暗号化ファイルの転送時や移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００３５】或いは本発明の暗号システムの他の態様では、前記全体暗号化手段は、第２公開鍵で前記部分暗号化ファイルを暗号化し、前記全体復号化手段は、前記第２公開鍵に対応する第２秘密鍵で前記全体暗号化ファイルを復号化する。

【００３６】この態様によれば、全体暗号化ファイルは、第２秘密鍵がなければ復号化できないので、当該全体暗号化ファイルの転送時や移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００３７】本発明の暗号システムの他の態様では、前記部分暗号化ファイルに対し、前記個人レコード毎に個人ＩＤコードとは異なるレコード識別子を付与する手段を更に含み、前記部分暗号化手段は、前記レコード識別子に基づいて前記個人レコードの統計処理又は解析処理が可能なように前記選択されたフィールドを暗号化する。

【００３８】この態様によれば、個人のプライバシーを保護したまま、部分暗号化ファイルを、個人レコード毎に付与されたレコード識別子に基づいて、統計処理又は解析処理が可能となり、各種データベースを構築することも可能となる。例えば、同じ値は同じ値に変える方式の暗号化方式であれば、暗号化された状態（個人を特定できない状態）のままで、各種統計処理や解析処理を行える。しかも、守秘義務のある関係機関や関係者によって、フィールドを部分的に暗号化した際に用いた第１公開鍵に対応する第１秘密鍵を用いて部分復号化処理を行えば、このように統計処理や解析処理の結果上における個人データを全て見ることも可能となる。

【００３９】本発明の暗号化装置は上記課題を解決するために、所定単位の個人データを統一フォーマットで項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる個人レコードを少なくとも一つ含んでなる個人データファイルの中で、所定基準に従って個人を特定可能とされる項目に対応するフィールドを選択する選択手段と、該選択されたフィールドを第１公開鍵で暗号化すると共に前記選択手段により選択されないフィールドを暗号化しないで部分暗号化ファイルを作成する部分暗号化手段と、該作成された部分暗号化ファイルを暗号化して全体暗号化ファイルを作成する全体暗号化手段とを備える。

【００４０】本発明の暗号化装置によれば、先ず選択手段により、複数フィールドからなる個人レコードを含んでなる個人データファイルの中で、所定基準に従って、個人を特定可能とされる項目に対応するフィールドを選択する。そして、部分暗号化手段により、このように選択されたフィールドを第１公開鍵で暗号化すると共に選択されないフィールドを暗号化しないことにより、部分

暗号化ファイルを作成する。続いて、全体暗号化手段により、この作成された部分暗号化ファイルを暗号化して、全体暗号化ファイルを作成する。その後、この全体暗号化ファイルが、インターネット等の通信手段を通じて転送されたり、記憶媒体に格納された状態で移送される際に、当該全体暗号化ファイルが漏洩したり盗難されたりしても、全体が暗号化されているので、意味が理解されることは無い。

【００４１】本発明の復号化装置は上記課題を解決するために、上述した本発明の暗号化装置により作成された全体暗号化ファイルを復号化して前記部分暗号化ファイルを再生する全体復号化手段を備える。

【００４２】本発明の復号化装置によれば、暗号化装置により作成された全体暗号化ファイルの転送或いは移送先である、例えば他の医療関連施設等で、全体復号化手段により、この全体暗号化ファイルを復号化して部分暗号化ファイルを再生する。従って本発明の復号化装置によれば、個人のプライバシーを守りながら、個人データの解析処理や統計処理を行うことが可能となる。

【００４３】本発明の復号化装置の一態様では、前記再生された部分暗号化ファイルのうち前記選択されたフィールドを前記第１公開鍵に対応する第１秘密鍵で復号化して前記個人データファイルを再生する部分復号化手段を更に備える。

【００４４】この態様によれば、部分復号化手段により、再生された部分暗号化ファイルのうち、未だ暗号化されているフィールドを、第１公開鍵に対応する第１秘密鍵で復号化して、個人データファイルを再生する。従って、当該個人データについて守秘義務のある特定人のみに第１秘密鍵を知らせておけば、この者のみが復号化後の個人データの全てを見ることができる。

【００４５】本発明の第１コンピュータプログラムは上記課題を解決するために、上述した本発明の暗号システム（但し、その各種態様も含む）として、コンピュータを機能させる。

【００４６】本発明の第１コンピュータプログラムによれば、当該コンピュータプログラムを格納するＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の記録媒体から、当該コンピュータプログラムをコンピュータに読み込んで実行させれば、或いは、当該コンピュータプログラムを通信手段を介してダウンロードさせた後に実行させれば、上述した本発明の暗号システムを比較的簡単に構築できる。

【００４７】本発明の第２コンピュータプログラムは上記課題を解決するために、上述した本発明の暗号化装置として、コンピュータを機能させる。

【００４８】本発明の第２コンピュータプログラムによれば、当該コンピュータプログラムを格納するＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の記録媒体から、当該コンピュータプログラムをコンピュータに読み込んで実行させれば、或いは、当該コンピュータプログラムを通信手段を介してダウンロードさせた後に実行させれば、上述した本発明の暗号化装置を比較的簡単に構築できる。

【００４９】本発明の第３コンピュータプログラムは上記課題を解決するために、上述した本発明の復号化装置として、コンピュータを機能させる。

【００５０】本発明の第３コンピュータプログラムによれば、当該コンピュータプログラムを格納するＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の記録媒体から、当該コンピュータプログラムをコンピュータに読み込んで実行させれば、或いは、当該コンピュータプログラムを通信手段を介してダウンロードさせた後に実行させれば、上述した本発明の復号化装置を比較的簡単に構築できる。

【００５１】本発明のこのような作用及び他の利得は次に説明する実施の形態から明らかにされよう。

【００５２】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

【００５３】（第１実施形態）先ず、本発明の第１実施形態に係る暗号システムの構成について図１を参照して説明する。図１は、第１実施形態に係る暗号システムのブロック図である。

【００５４】図１において、暗号システムは、暗号化装置１００ａ、記憶装置１１０、通信手段１３１及び２３１、第１復号化装置２００ａ、処理装置２４０、記憶装置２５０並びに第２復号化装置３００を備えて構成されている。

【００５５】記憶装置１１０内には、所定単位の患者データを統一フォーマットで、医療関連項目毎に夫々コード化、デジタル化又はテキスト化した複数フィールドからなる患者レコードを複数含んでなる患者データファイル１１１が構築されている。ここに「患者レコード」とは、１入院単位、１レセプト単位、１カルテ単位等の患者データを取り扱う上でまとめられた記録の単位である。

【００５６】暗号化装置１００ａは、フィールド選択手段１０１、部分暗号化手段１０２、全体暗号化手段１０３を備える。これらの手段は、例えば暗号化装置１００ａを構成するコンピュータのＣＰＵ（Central Processing Unit）内に論理的に構築される。暗号化装置１００ａは更に、キーボード、マウス、スイッチ、カードリーダ等の入力手段１０４を備える。入力手段１０４を介して、第１公開鍵及び共通鍵が入力される。

【００５７】フィールド選択手段１０１は、記憶装置１１０内に構築されている患者データファイル１１１の中で、所定基準に従って、患者個人を特定可能とされる項目に対応するフィールドを選択するように構成されている。ここでは、例えば患者氏名に対応するフィールド、患者ＩＤに対応するフィールド、患者の生年月日に対応するフィールド、退院年月日に対応するフィールド、入院年月日に対応するフィールドなど、患者を特定可能と

される項目に対応するフィールドを選択する。このような患者個人等の個人を特定可能か否かについての所定基準は、経験的、実験的、理論的に予め設定されている。

【００５８】部分暗号化手段１０２は、フィールド選択手段１０１により選択されたフィールドを、入力手段１０４を介して入力された第１公開鍵を用いて、公開鍵方式により暗号化すると共に、フィールド選択手段１０１により選択されないフィールドを暗号化しないことにより、部分暗号化ファイル１１２を記憶装置１１０内に作成するように構成されている。

【００５９】全体暗号化手段１０３は、記憶装置１１０内に作成された部分暗号化ファイル１１２を、入力手段１０４を介して入力された共通鍵を用いて、共通鍵方式により暗号化して、全体暗号化ファイル１１３を記憶装置１１０内に作成するように構成されている。

【００６０】通信手段１３１は、記憶装置１１０内に作成された全体暗号化ファイル１１３を、所定プロトコルによりインターネット１５０経由で通信手段２３１に送信するように構成されている。

【００６１】他方、通信手段２３１は、このような暗号化後に送信された全体暗号化ファイル１１３を、所定プロトコルによりインターネット経由で受信するように構成されている。

【００６２】尚、このような通信回線として、インターネット１５０に限らず、有線、無線、専用回線、一般回線等の種類を問わずに各種回線に対して、本実施形態は適用可能である。

【００６３】他方、第１復号化装置２００ａは、全体復号化手段２０３を備える。この手段は、例えば第１復号化装置２００ａを構成するコンピュータのＣＰＵ内に論理的に構築される。第１復号化装置２００ａは更に、キーボード、マウス、スイッチ、カードリーダ等の入力手段２０４を備える。入力手段２０４を介して、暗号化装置１００ａ側で入力手段１０４に入力された共通鍵と同じ共通鍵が入力される。

【００６４】全体復号化手段２０３は、通信手段２３１が受信した全体暗号化ファイルを、入力手段２０４を介して入力された共通鍵を用いて復号化し、部分暗号化ファイルを再生するように構成されている。そして、処理手段２４０は、このように再生された部分暗号化ファイルに対して、各患者レコードに識別子を付与する処理や、所定規則に従って分類する処理或いは変換する処理など各種のデータ処理を行って、医療情報データベース２５１を記憶装置２５０内に創生する。

【００６５】このように創生される医療情報データベース２５１は、これを格納する記憶装置２５０に接続された複数のパソコン、ワークステーション等の端末装置３１０において、症例分析、病院評価、術式評価、投薬評価等の各種の統計処理や解析処理に供される。そして特に、このように記憶装置２５０に接続された複数の端末装置のうちの少なくとも一つである端末装置３１０Ｓは、第２復号化装置３００を備えて構成されている。

【００６６】第２復号化装置３００は、部分復号化手段３０２を備える。この手段は、例えば第２復号化装置３００を構成するコンピュータのＣＰＵ内に論理的に構築される。第２復号化装置３００は更に、キーボード、マウス、スイッチ、カードリーダ等の入力手段３０４を備える。入力手段３０４を介して、暗号化装置１００ａ側で入力手段１０４に入力された第１公開鍵に対応する第１秘密鍵が入力される。

【００６７】部分復号化手段３０２は、医療情報データベース２５１に格納された部分暗号化ファイルを復号化して、暗号処理の施されていない患者データファイルを再生可能に構成されている。

【００６８】次に図２から図６を参照して、以上の如く構成された第１実施形態に係る暗号システムにおける暗号方法について説明する。

【００６９】先ず図２及び図３を参照して、暗号化方法について説明する。ここに図２は、当該暗号化方法のフローチャートであり、図３は、患者データファイル１１１に含まれる各レコードが暗号化される様子を示す概念図である。

【００７０】図２において、先ず複数フィールドからなる患者レコードを含んでなる患者データファイル１１１の中で、予め設定された患者個人を特定可能とされる項目に対応するフィールドを選択する（ステップＳ１１）。ここでは例えば、図３の上段に示すように、患者データファイル１１１を構成するデータテーブル１１１ａにおいて、患者ＩＤに対応するフィールド、退院日に対応するフィールド、入院日に対応するフィールド等を選択する。

【００７１】再び図２において、このステップＳ１１と相前後して、部分暗号化に用いる第１公開鍵を入力手段１０４を介して取得する（ステップＳ１２）。続いて、ステップＳ１１で選択された、患者レコード中のフィールドを、ステップＳ１２で取得した第１公開鍵で暗号化する。そして、ステップＳ１２で選択されない、患者レコード中のフィールドを暗号化しないことにより、部分暗号化ファイル１１２を作成する（ステップＳ１３）。ここでは例えば、図３の上半分に示すように、患者データファイル１１１を構成するデータテーブル１１１ａにおいて、患者ＩＤに対応するフィールド、退院日に対応するフィールド、入院日に対応するフィールド等が、第１公開鍵により暗号化された、部分暗号化ファイル１１２を構成するデータテーブル１１２ａを作成する。

【００７２】再び図２において、これらステップＳ１１からＳ１３と相前後して、全体暗号化に用いる共通鍵を入力手段１０４を介して取得する（ステップＳ１４）。続いて、ステップＳ１３で作成された部分暗号化ファイル１１２を、ステップＳ１４で取得した共通鍵を用いた

共通鍵方式で暗号化して、全体暗号化ファイル１１３を作成する（ステップＳ１５）。ここでは例えば、図3の下半分に示すように、部分暗号化ファイル１１２を構成するデータテーブル１１２ａにおいて、全フィールドが共通鍵により暗号化された、全体暗号化ファイル１１３を構成するデータテーブル１１３ａを作成する。

【００７３】再び図2において、このように作成された全体暗号化ファイル１１３を、インターネット１５０を通じて、通信手段１３１から通信手段２３１に送信して（ステップＳ１６）、一連の処理を終える。ここでは、例えば病院などの一の医療関連施設に設置された暗号化装置１００ａから、医療研究所などの他の医療関連施設に設置された第１復号化装置２００ａに転送される。この際、全体暗号化ファイル１１３が、送信の途中で漏洩したり盗難されたりしても、全体が暗号化されているので、意味が理解されることはない。

【００７４】次に図４から図６を参照して、本実施形態の暗号方法における復号化方法について説明する。ここに図４は、当該復号化方法のフローチャートであり、図５は、患者データファイルに含まれる各レコードが復号化される様子を示す概念図であり、図６は、暗号化されたデータコードが復号化される一具体例を示す概念図である。

【００７５】図４において先ず、通信手段２３１により、インターネット１５０を介して、通信手段１３１から送信された全体暗号化ファイルを受信する（ステップＳ２１）。このステップＳ２１と相前後して、第１復号化装置２００ａにおける全体復号化に用いる共通鍵、即ち暗号化装置１００ａにおける全体暗号化手段１０３で用いた共通鍵と同じ鍵を、入力手段２０４を介して取得する（ステップＳ２２）。

【００７６】続いて、ステップＳ２１で受信した全体暗号化ファイルを、ステップＳ２２で取得した共通鍵を用いた共通鍵方式で復号化して、部分暗号化ファイルを作成する（ステップＳ２３）。ここでは例えば、図５の上半分に示すように、全フィールドが暗号化された全体暗号化ファイル１１３を構成するデータテーブル１１３ａを、共通鍵方式で全体復号化することにより、部分暗号化ファイル１１２を構成するデータテーブル１１２ａを作成する。即ち、このように復号化しても、図２のステップＳ１３で部分暗号化された、患者ＩＤに対応するフィールド、退院日に対応するフィールド、入院日に対応するフィールド等は、意味が理解されることはない。

【００７７】次に、このように患者個人を特定可能とされた項目を除いて復号化された患者データに基づいて、データベースを創生する（ステップＳ２４）。ここでは、例えば、図５の中段に示すように、ステップＳ２３で部分的に復号化された部分暗号化ファイル１１２を構成するデータテーブル１１２ａに対し、個人ＩＤコードとは異なる識別子として、データＮｏ．を新たに付与する。そして、患者ＩＤ、入院日、退院日、生年月日等については、暗号化されたままテーブル２５１ａの一部として医療情報データベース２５１に組み込まれる。本実施形態では特に、暗号化装置１００ａ側の部分暗号化手段１０２による部分暗号化は、識別子たるデータＮｏ．に基づいて患者レコードの統計処理又は解析処理が可能なように、同じコードは同じコードに変換し、同じデジタル値は同じデジタル値に変換し、或いは同じテキストは同じテキストに変換する可逆方式の暗号化方式により行われている。他方、患者個人を特定可能でないとされた最終採番日、最終更新日については、暗号化されていない形で、テーブル２５１ａの一部として医療情報データベース２５１に組み込まれる。

【００７８】再び図４において、各端末装置３１０では、その入力手段を介して、暗号化装置１００ａ側の入力手段１０４を介して入力された第１公開鍵に対応する第１秘密鍵が入力されたか否かが判定される（ステップＳ２５）。例えば、端末装置３１０Ｓで入力手段３０４を介して第１秘密鍵が入力されると（ステップＳ２５：はい）、このステップＳ２５で取得された第１秘密鍵を用いた公開鍵方式により、医療情報データベース２５１に暗号化されたまま含まれる患者データの特定フィールドは、復号化される（ステップＳ２６）。ここでは例えば、図５の下半分に示すように、医療情報データベース２５１を構成するデータテーブル２５１ａにおいて、患者ＩＤに対応するフィールド、退院日に対応するフィールド、入院日に対応するフィールド等が、第１秘密鍵により復号化された、患者データファイル１１１を構成するデータテーブル１１１ａを作成する。より具体的には、図６の上段に示すように、暗号化されており意味不明な患者ＩＤ（Ａ２欄）、退院日（Ａ３欄）、入院日（Ａ４欄）等を、図６の下段に示すように、意味が分かる退院日、入院日等に復号化する。

【００７９】再び図４において、ステップＳ２６における復号化の後、又はステップＳ２５で第１秘密鍵が入力されなければ（ステップＳ２５：いいえ）、例えば病院評価、症例分析、術式評価、投薬評価等の統計処理や解析処理を行って（ステップＳ２７）、一連の処理を終了する。

【００８０】以上説明した暗号化方法及び復号化方法を用いれば、転送先である、例えば研究施設、公的機関、他の病院、大学等の他の医療関連施設で、全体暗号化ファイルを復号化して部分暗号化ファイルを再生しても、患者個人を特定可能とされるフィールドが、未だ第１公開鍵で暗号化された状態にある。従って、当該他の医療関連施設で一般に守秘義務のない研究員、調査員、事務員等がこのような部分暗号化ファイルの一部として、患者データを見ても、これに係る患者個人が特定されてしまうことは殆どない。この際特に、患者個人を特定可能とされる項目についての基準を調節することにより、患

者個人が特定されることを避けつつ、患者データを各種解析や統計処理に利用できる。例えば、患者が、今までに何回入院したのか？以前に入院したのか？以前にどのような治療をしたのか？などの情報は、暗号化されていないフィールドを見れば、患者個人を特定することなく分かる。

【００８１】特に、患者個人を特定しないままで、暗号化されたデータを統計処理や解析処理し、それらの処理結果については（患者個人を特定し難い性質を持つので）暗号化しないようにするのが好ましい。このように、ある患者データについて患者個人を特定可能な状態では暗号化しつつ統計処理等に用いることにより、プライバシーの保護を図りつつ患者データの医療向上への有効利用を図れる。

【００８２】更に本実施形態によれば、第２復号化装置３００があれば、部分暗号化ファイルを、第１秘密鍵を用いて復号化して患者データファイルを完全に再生することもできる。このため、患者データについて守秘義務のある、例えば主治医等の特定人のみに第１秘密鍵を知らせておけば、この者のみが復号化後の個人データの全てを見ることができる。

【００８３】尚、以上説明した実施形態では、各患者レコードにおけるフィールドを、単純に部分暗号化するか又はしないかに分けたが、段階的な複数の基準に従ってフィールドを段階的に選択して部分暗号化することも可能である。例えば、患者個人を特定するのが非常に容易な、患者氏名、患者住所、患者ＩＤなどについては第１基準とし、生年月日、入院月日、退院月日等については第２基準とし、入院期間、病歴、慢性病歴等については第３基準として、フィールドを段階毎に異なる第１公開鍵で暗号化する。そして、第２復号化装置３００において、段階的に選択されたフィールドを段階毎に異なる第１公開鍵に対応する第１秘密鍵で復号化するように構成すれば、復号化後の部分暗号化ファイルを、例えば所長、副所長、事務委員長、研究者、事務員等の立場が異なる人間に対して異なる第１秘密鍵を知らせることにより、その立場に応じて見るようにできる。

【００８４】（第２実施形態）次に、本発明の第２実施形態に係る暗号システムについて図７から図９を参照して説明する。

【００８５】先ず、本発明の第２実施形態に係る暗号システムの構成について図７を参照して説明する。図７は、第２実施形態に係る暗号システムのブロック図である。尚、図７において、図１に示した第１実施形態と同様の構成要素には同様の参照符号を付し、それらの説明は省略する。

【００８６】図７において、暗号システムは、暗号化装置１００ｂ、記憶装置１１０、通信手段１３１及び２３１、第１復号化装置２００ｂ、処理装置２４０、記憶装置２５０並びに第２復号化装置３００を備えて構成されている。暗号化装置１００ｂは、フィールド選択手段１０１、部分暗号化手段１０２、全体暗号化手段１０３及び入力手段１０４に加えて、共通鍵を第２公開鍵を用いて暗号化する共通鍵暗号化手段１０６を備える。そして、入力手段１０４を介して入力された共通鍵は、第２公開鍵を用いて共通鍵暗号化手段１０６により暗号化されて通信手段１３１により、全体暗号化ファイル１１３と共に送信される。他方、第１復号化装置２００ｂは、全体復号化手段２０３及び入力手段２０４に加えて、通信手段２３１により全体暗号化ファイルと共に受信した共通鍵を、第２秘密鍵を用いて復号化する共通鍵復号化手段２０６を備える。その他の構成については、上述した第１実施形態の場合と同様である。

【００８７】次に図８及び図９を参照して、以上の如く構成された第２実施形態に係る暗号システムにおける暗号方法について説明する。

【００８８】先ず図８を参照して、暗号化方法について説明する。ここに図８は、当該暗号化方法のフローチャートである。尚、図８において、図２に示した第１実施形態と同様のステップについては同様のステップ番号を付し、それらの説明は省略する。

【００８９】図８において、第１実施形態の場合と同様にステップＳ１１からＳ１５までの処理が行われる。次に、入力手段１０４或いは他の入力手段を介して第２公開鍵を取得する（ステップＳ３１）。続いて、共通鍵暗号化手段１０６によって、ステップＳ３１で所得した第２公開鍵を用いて、ステップＳ１４で取得した共通鍵を暗号化する（ステップＳ３２）。その後、ステップＳ１５で作成された全体暗号化ファイル１１３とステップＳ３２で暗号化した共通鍵とを、インターネット１５０を通じて、通信手段１３１から通信手段２３１に送信して（ステップＳ３３）、一連の処理を終える。

【００９０】次に図９を参照して、本実施形態の暗号方法における復号化方法について説明する。ここに図９は、当該復号化方法のフローチャートである。尚、図９において、図４に示した第１実施形態と同様のステップについては同様のステップ番号を付し、それらの説明は省略する。

【００９１】図９において先ず、通信手段２３１により、インターネット１５０を介して、通信手段１３１から送信された全体暗号化ファイルと暗号化された共通鍵とを受信する（ステップＳ４１）。続いて、入力手段２０４を介して、暗号化装置１００ｂにおける共通鍵暗号化手段で用いた第２公開鍵に対応する第２秘密鍵を取得し（ステップＳ４２）、この取得した第２秘密鍵を用いて共通鍵復号化手段２０６により、共通鍵の復号化を行う（ステップＳ４３）。

【００９２】その後は、この復号化された共通鍵を用いて、上述した第１実施形態と同様にステップＳ２２からＳ２７の処理が行われる。

【００９３】以上詳細に説明したように第２実施形態によれば、全体暗号化ファイル１１３の作成時に用いた共通鍵は、第２公開鍵で暗号化されていることとなり、当該全体暗号化ファイル１１３の転送時や移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００９４】（第３実施形態）次に、本発明の第３実施形態に係る暗号システムについて図１０を参照して説明する。図１０は、第３実施形態に係る暗号システムのブロック図である。尚、図１０において、図１に示した第１実施形態と同様の構成要素には同様の参照符号を付し、それらの説明は省略する。

【００９５】図１０において、暗号システムは、暗号化装置１００ａ’側では、共通鍵ではなく第２公開鍵が入力手段１０４に入力され、全体暗号化手段１０３’により共通鍵方式ではなく公開鍵方式で暗号化を行い、これに対応して、第１復号化装置２００ａ’側では、共通鍵ではなく第２秘密鍵が入力手段２０４に入力され、全体復号化手段２０３’により共通鍵方式ではなく公開鍵方式で復号化を行うように構成されている。更に、通信手段１３１ではなく、フレキシブルディスクドライブ、ＣＤ−ＲＡＭドライブ、ＤＶＤ−ＲＡＭドライブ等の書込手段１３２を備え、通信手段２３１ではなく、フレキシブルディスクドライブ、ＣＤドライブ、ＤＶＤドライブ等の読取手段２３２を備える。その他の構成については、上述した第１実施形態の場合と同様である。

【００９６】従って、第３実施形態によれば、公開鍵方式によって暗号化した全体暗号化ファイル１１３’は、第２秘密鍵がなければ復号化できないので、当該全体暗号化ファイル１１３’を格納する記録媒体１６０の移送時における漏洩、盗難に対するセキュリティーを向上できる。

【００９７】（第４実施形態）次に、本発明の第４実施形態に係る暗号システムについて説明する。

【００９８】第４実施形態では、上述した第１から第３実施形態の構成において、第１秘密鍵或いは第２秘密鍵を構成するデータが少なくとも二つに分割されており、その他の構成については、上述した第１から第３実施形態と同様である。

【００９９】従って、秘密鍵（第１或いは第２秘密鍵）を秘密鍵片として二者で保持することが可能となる。同時に、一者が保持する秘密鍵片だけでは、秘密鍵としての本来の機能を発揮できないので、物理的に離れた二者により別個に保持される秘密鍵片の片方が、盗難にあっても、暗号化ファイルを復号化できない。この結果、セキュリティレベルが格段に上昇する。そして特に、このように秘密鍵（第１或いは第２秘密鍵）を二つに分割する場合、秘密鍵片の片方を保持する者が、この秘密鍵片をコピー等して複数作成して保持しておくようにすれば、全てのコピー及びオリジナルを一時に紛失或いは破壊してしまう可能性は格段に低くなる。即ち、全体としてみれば、秘密鍵を紛失する可能性が非常に低くなる。他方で、複数或いは多数コピーすることで秘密鍵片が漏洩する可能性自体が高まっても、秘密鍵としての機能を果たさない秘密鍵片である限りにおいて、漏洩或いは盗難による実用上の問題は殆ど生じない。

【０１００】以上のように第４実施形態により、盗難、漏洩、紛失或いは破壊に対して、非常に強い暗号システムが構築可能とされる。

【０１０１】（第５実施形態）次に、本発明の第５実施形態に係る暗号システムについて説明する。

【０１０２】第５実施形態では、上述した第４実施形態の構成において、段階的な複数の基準に従ってフィールドを段階的に選択して部分暗号化しておく。例えば、患者個人を特定するのが非常に容易な、患者氏名、患者住所、患者ＩＤなどについては第１基準とし、生年月日、入院月日、退院月日等については第２基準とし、入院期間、病歴、慢性病歴等については第３基準として、フィールドを段階毎に異なる公開鍵で暗号化する。そして、秘密鍵片が、いずれかの段階的な公開鍵に対応する秘密鍵に一致するように、秘密鍵及び秘密鍵片を構成する。その他の構成については、上述した第４実施形態と同様である。

【０１０３】従って、秘密鍵片を集めることで、秘密鍵が得られて、患者データファイルを完全に復号化可能なように暗号システムを構築でき、同時に、秘密鍵片を管理レベル分けされた段階的な秘密鍵として用いることで、管理レベルに応じたフィールドのみを復号化可能となる。

【０１０４】以上のように第５実施形態によれば、秘密鍵を分割することにより、盗難、漏洩、紛失或いは破壊に対して、非常に強い暗号システムが得られると共に、秘密鍵片を管理レベルに対応させることにより、秘密鍵片を段階的な秘密鍵として用いることが可能な暗号システムが構築可能とされる。

【０１０５】以上説明した第１から第５実施形態では、暗号化装置１００ａ，１００ｂ及び１００ａ’、第１復号化装置２００ａ、２００ｂ及び２００ａ’、並びに第２復号化装置３００は夫々、パーソナルコンピュータ、ワークステーション、モバイルコンピュータ等のコンピュータから構成されてもよい。この場合、各コンピュータを夫々の暗号化装置、第１復号化装置又は第２復号化装置として機能させるコンピュータプログラムを格納するＣＤ−ＲＯＭ、ＤＶＤ−ＲＯＭ等の記録媒体から、当該コンピュータプログラムをコンピュータに読み込んで実行させれば、或いは、当該コンピュータプログラムを通信手段を介してダウンロードさせた後に実行させれば、上述した実施形態における暗号化装置１００ａ，１００ｂ及び１００ａ’、第１復号化装置２００ａ、２００ｂ及び２００ａ’、並びに第２復号化装置３００を夫々比較的簡単に構築できる。

【０１０６】また、上述した実施形態における公開鍵暗

号方式としては、例えばＲＳＡ暗号等の公知の暗号方式を採用可能であり、共通鍵或いは秘密鍵暗号方式としては、例えばＭＩＳＴＹ暗号、ＤＥＳ暗号等の格子の暗号方式を採用可能である。

【０１０７】加えて、上述した各実施形態においては、暗号化の対象たる患者データファイルは、論理構造を有する固定長の或いは文書型定義を持つデータファイルであってもよい。又は、論理構造を有するものの、可変長の或いは文書型定義を持たないデータファイルであってもよい。例えば、患者データファイルは、文書型定義を持たないＸＭＬ文書からなってもよい。この場合、暗号化されたデータの先頭部分等に、各フィールドの管理レベルを示す管理情報を持たせると共に、ＩＣカード等に記憶されており且つ管理レベルを持つ秘密鍵を用いて、管理レベルに対応するフィールドを管理情報に基づいて復号化する構成とするのが好ましい。このように構成すれば、患者データファイルに、文書型定義が存在しなくても、復号化する際に特に支障は生じないで済む。更に秘密鍵片を段階的な秘密鍵として用いて、文書型定義を持たないデータファイルにおける特定フィールドのみを復号化可能な暗号システムが得られる。

【０１０８】本発明は、上述した実施形態に限られるものではなく、請求の範囲及び明細書全体から読み取れる発明の要旨或いは思想に反しない範囲で適宜変更可能であり、そのような変更を伴なう暗号方法、暗号システム、暗号化装置、復号化装置及びコンピュータプログラムもまた本発明の技術的範囲に含まれるものである。

【０１０９】

【発明の効果】以上詳細に説明したように、本発明によれば、個人のプライバシーを守りながら、患者データ等の個人データの解析処理や統計処理を行うことが可能となり、最終的には個人データを医療等の各種産業で有効利用できる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る暗号システムのブロック図である。

【図２】第１実施形態における暗号化方法のフローチャートである。

【図３】第１実施形態における患者データファイルに含まれる各レコードが暗号化される様子を示す概念図である。

【図４】第１実施形態における復号化方法のフローチャートである。

【図５】第１実施形態における患者データファイルに含まれる各レコードが復号化される様子を示す概念図である。

【図６】第１実施形態における暗号化されたデータコードが復号化される一具体例を示す概念図である。

【図７】本発明の第２実施形態に係る暗号システムのブロック図である。

【図８】第２実施形態における暗号化方法のフローチャートである。

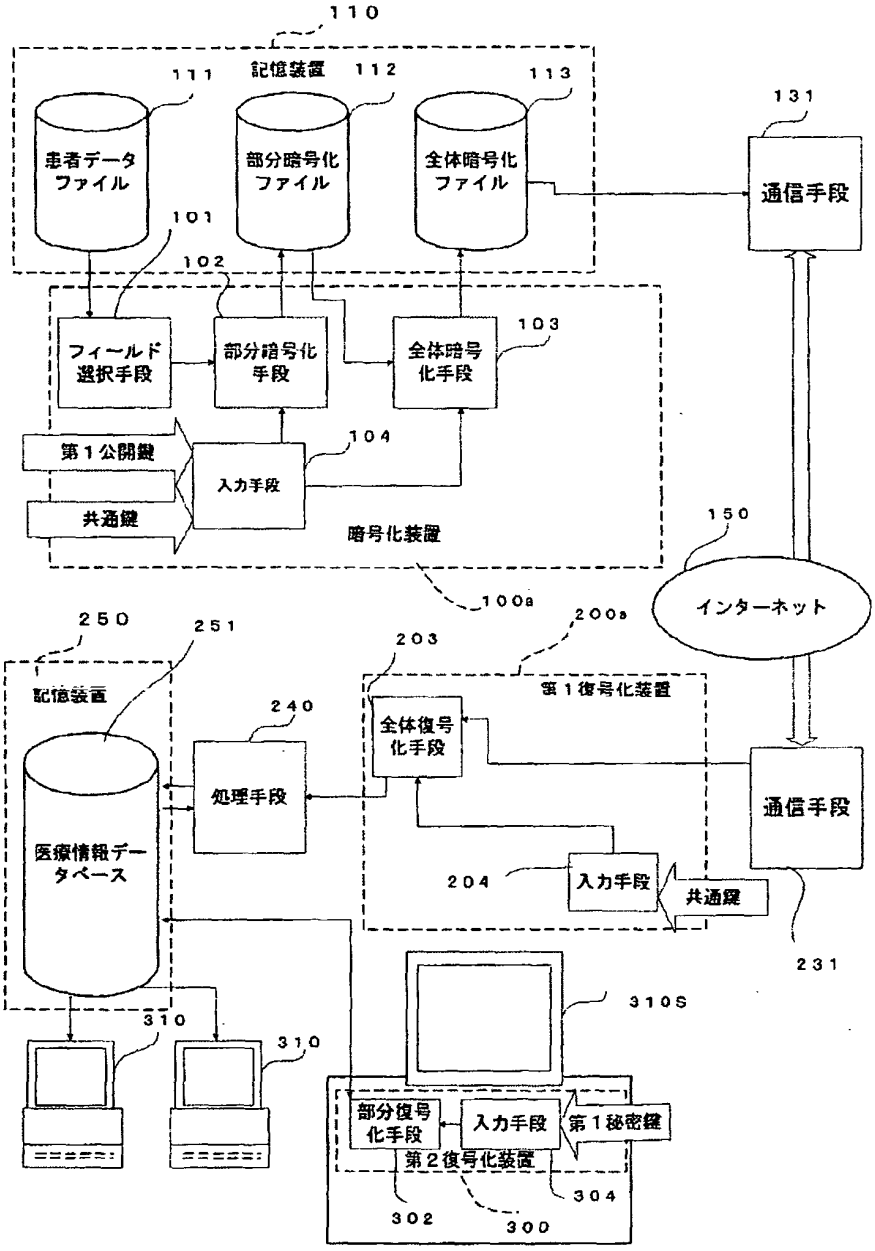
【図９】第２実施形態における復号化方法のフローチャートである。

【図１０】本発明の第３実施形態に係る暗号システムのブロック図である。

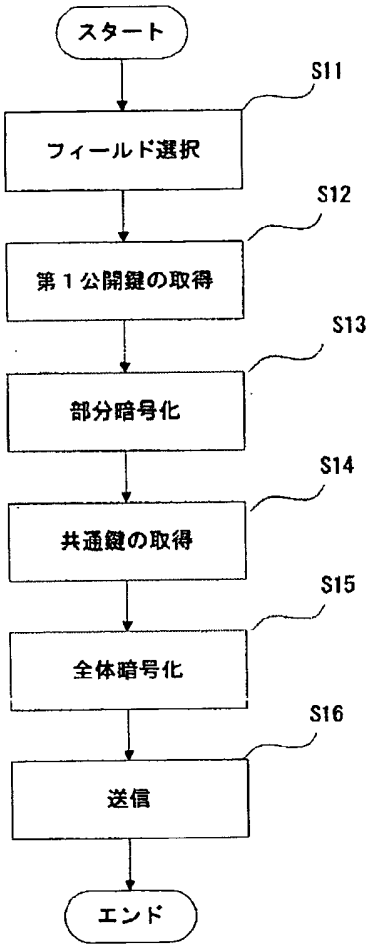
【符号の説明】

１００ａ、１００ｂ、１００ａ’…暗号化装置
１０１…フィールド選択手段
１０２…部分暗号化手段
１０３…全体暗号化手段
１０４…入力手段
１０６…共通鍵暗号化手段
１１１…患者データファイル
１１２…部分暗号化ファイル
１１３、１１３’…全体暗号化ファイル
２００ａ、２００ｂ、２００ａ’…復号化装置
２０３、２０３’…全体復号化手段
２０４…入力手段
２０６…共通鍵復号化手段
２４０…処理手段
２５０…記憶装置
２５１…医療情報データベース
３００…第２復号化装置
３０２…部分復号化手段
３０４…入力手段

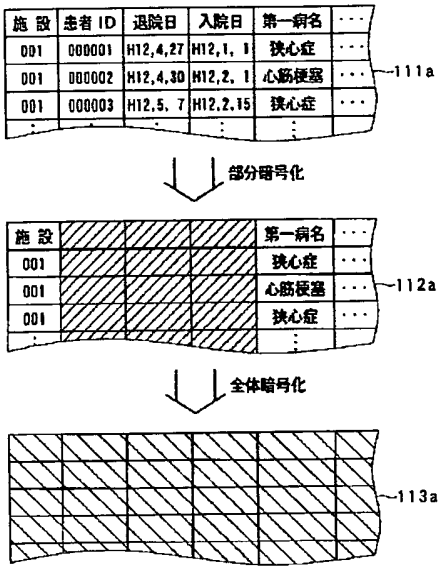
【図1】


110
記憶装置
111
患者データファイル
112
部分暗号化ファイル
113
全体暗号化ファイル
131
通信手段
101
102
フィールド選択手段
部分暗号化手段
全体暗号化手段
103
第１公開鍵
共通鍵
入力手段
104
暗号化装置
100a
150
インターネット
250
251
記憶装置
医療情報データベース
240
処理手段
200a
203
第１復号化装置
全体復号化手段
通信手段
204
入力手段
共通鍵
231
310S
310
310
部分復号化手段
入力手段
第１秘密鍵
第２復号化装置
304
302
300

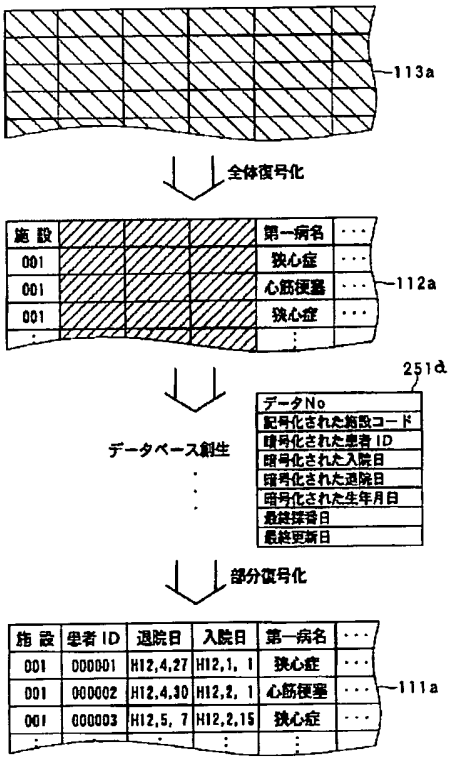
【図2】


スタート
S11
フィールド選択
S12
第１公開鍵の取得
S13
部分暗号化
S14
共通鍵の取得
S15
全体暗号化
S16
送信
エンド

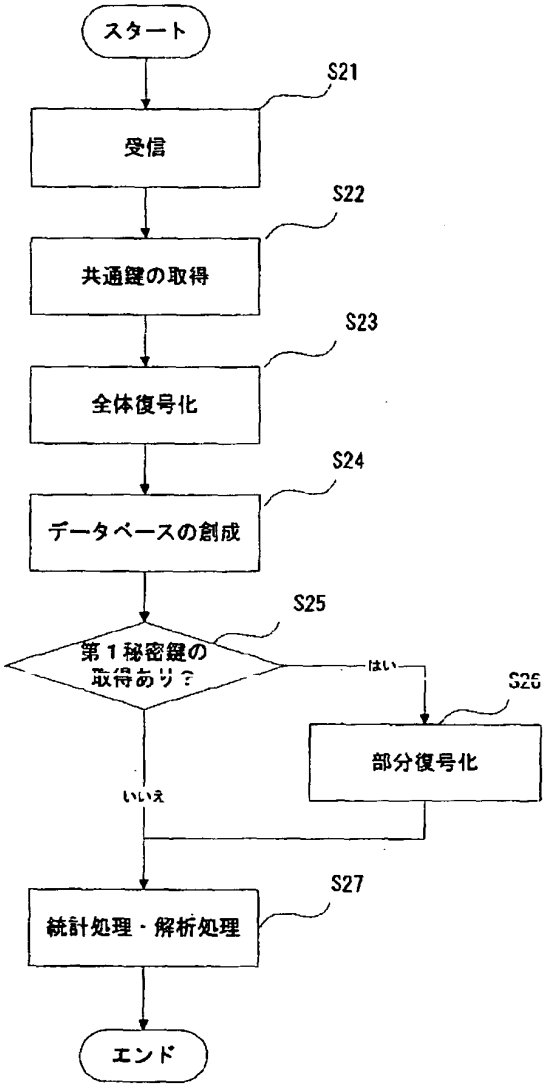
【図3】


施設 患者ID 退院日 入院日 第一病名
001 000001 H12,4,27 H12,1, 1 狭心症
001 000002 H12,4,30 H12,2, 1 心筋梗塞
001 000003 H12,5, 7 H12,2,15 狭心症
111a
部分暗号化
施設 第一病名
001 狭心症
001 心筋梗塞
001 狭心症
112a
全体暗号化
113a

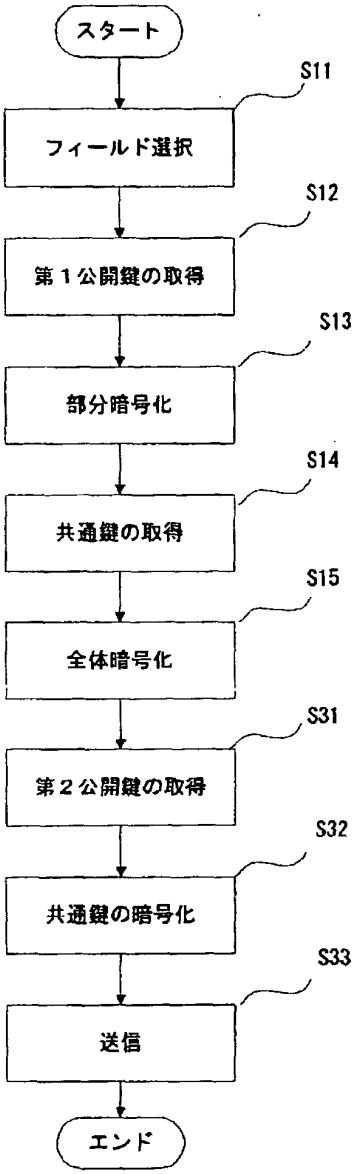
【図5】


113a
全体復号化
施設 第一病名
001 狭心症
001 心筋梗塞
001 狭心症
112a
251d
データNo
記号化された施設コード
暗号化された患者ID
暗号化された入院日
暗号化された退院日
暗号化された生年月日
最終採番日
最終更新日
データベース創生
部分復号化
施設 患者ID 退院日 入院日 第一病名
001 000001 H12,4,27 H12,1, 1 狭心症
001 000002 H12,4,30 H12,2, 1 心筋梗塞
001 000003 H12,5, 7 H12,2,15 狭心症
111a

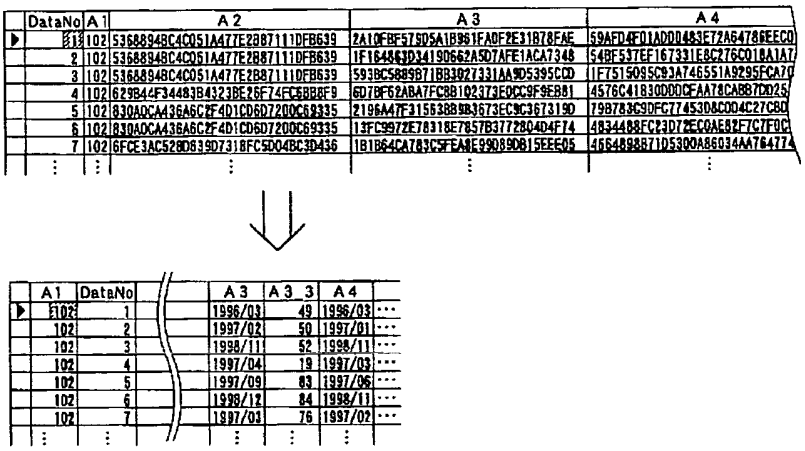
【図4】


スタート
S21
受信
S22
共通鍵の取得
S23
全体復号化
S24
データベースの創成
S25
第１秘密鍵の取得あり？
はい
S26
部分復号化
いいえ
S27
統計処理・解析処理
エンド

【図8】


スタート
S11
フィールド選択
S12
第１公開鍵の取得
S13
部分暗号化
S14
共通鍵の取得
S15
全体暗号化
S31
第２公開鍵の取得
S32
共通鍵の暗号化
S33
送信
エンド

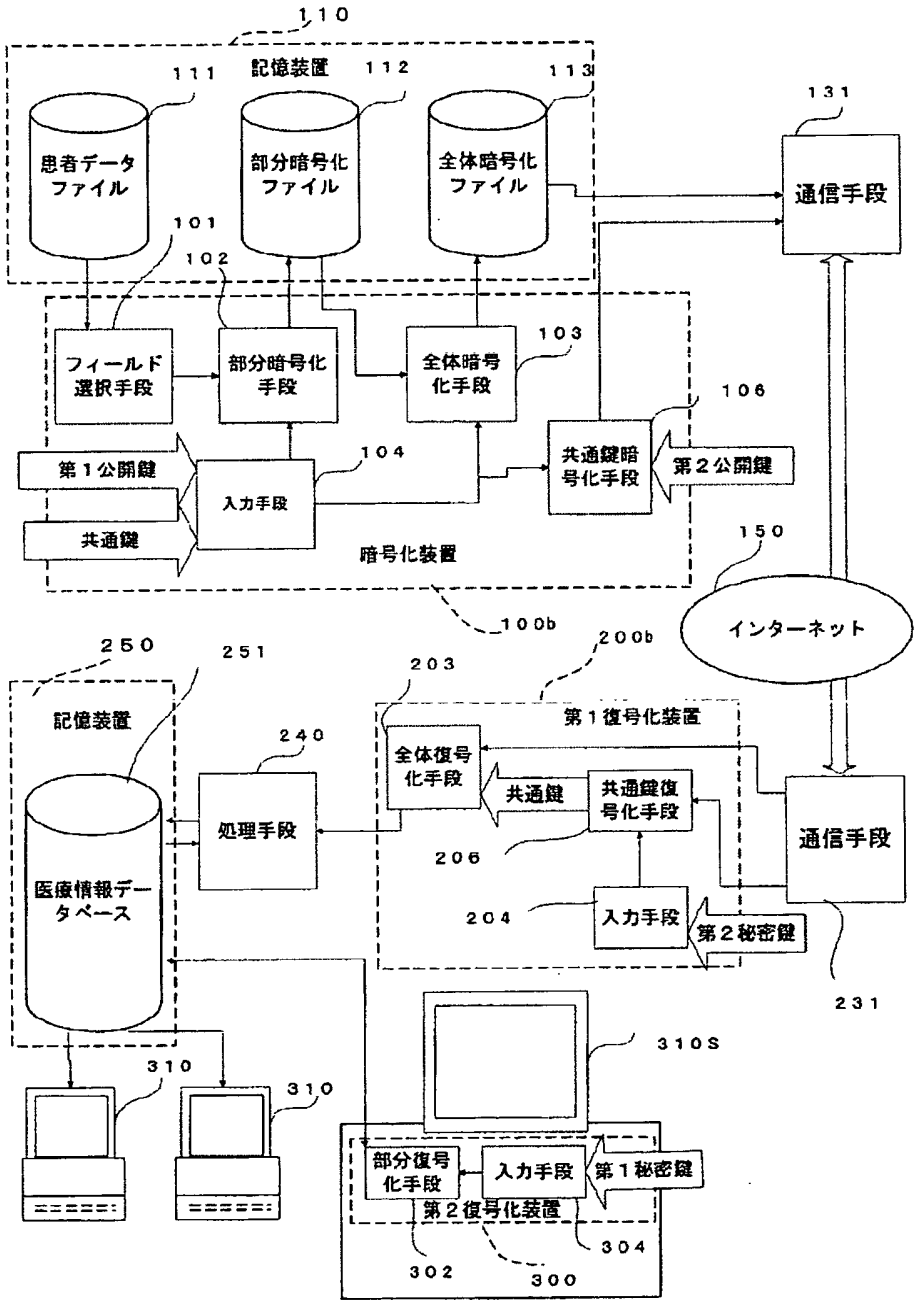
【図6】



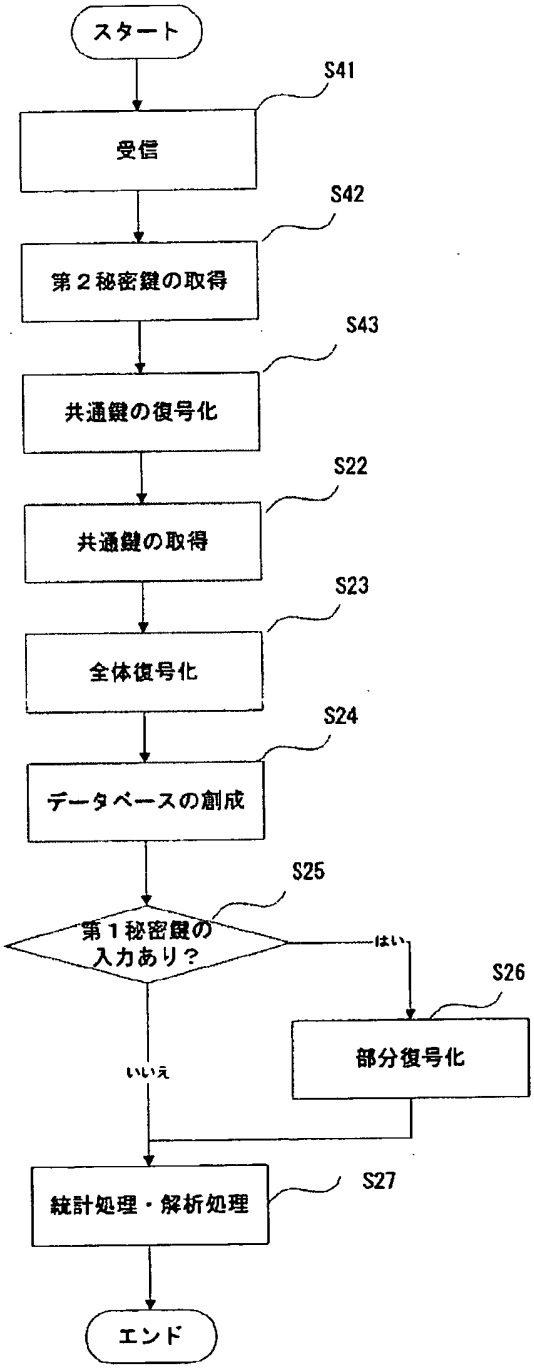
	DataNo	A1	A2	A3	A4
▶	1	102	53688948C4C051A477E2887111DFB639	2A10FBF575D5A1B961FA0F2E31B78FAE	59AFD4F01ADDD483E72A64786EEC0
	2	102	53688948C4C051A477E2887111DFB639	1F16484[illegible]D3419D662A5D7AFE1ACA7348	54BF537EF16733[illegible]E8C276C018A1A7
	3	102	53688948C4C051A477E2887111DFB639	593BC5889B71BB3927331AA9D5395CDD	1FF7515095C93A746551A9295FCA70
	4	102	629B44F34483B4323BE26F74FC6BB8F9	6D7BF62ABA7FC3B1023737E0CC9F9EB81	4576C41830D0DCFAA78CAB87D025
	5	102	830A0CA436A6C2F4D1CD6D7200C69335	2196A47F3156388[illegible]3673EC9C3673190	79B783C9DFC774530BCDD4C27CBD
	6	102	830A0CA436A6C2F4D1CD6D7200C69335	13FC9972E78318E7B57B3772B04D4F74	4834488FC23D72EC0AE82F7C7F0C
	7	102	6FCE3AC528D8399D7318FC5D04BC3D436	1B1B64CA783C9FEA8E99089D815EEE05	46648988710D5300A86034AA764774
	⋮	⋮	⋮	⋮	⋮

	A1	DataNo		A3	A3_3	A4	
▶	102	1		1996/03	49	1996/03	…
	102	2		1997/02	50	1997/01	…
	102	3		1998/11	52	1998/11	…
	102	4		1997/04	19	1997/03	…
	102	5		1997/09	83	1997/06	…
	102	6		1998/12	84	1998/11	…
	102	7		1997/03	76	1997/02	…
	⋮	⋮		⋮	⋮	⋮	

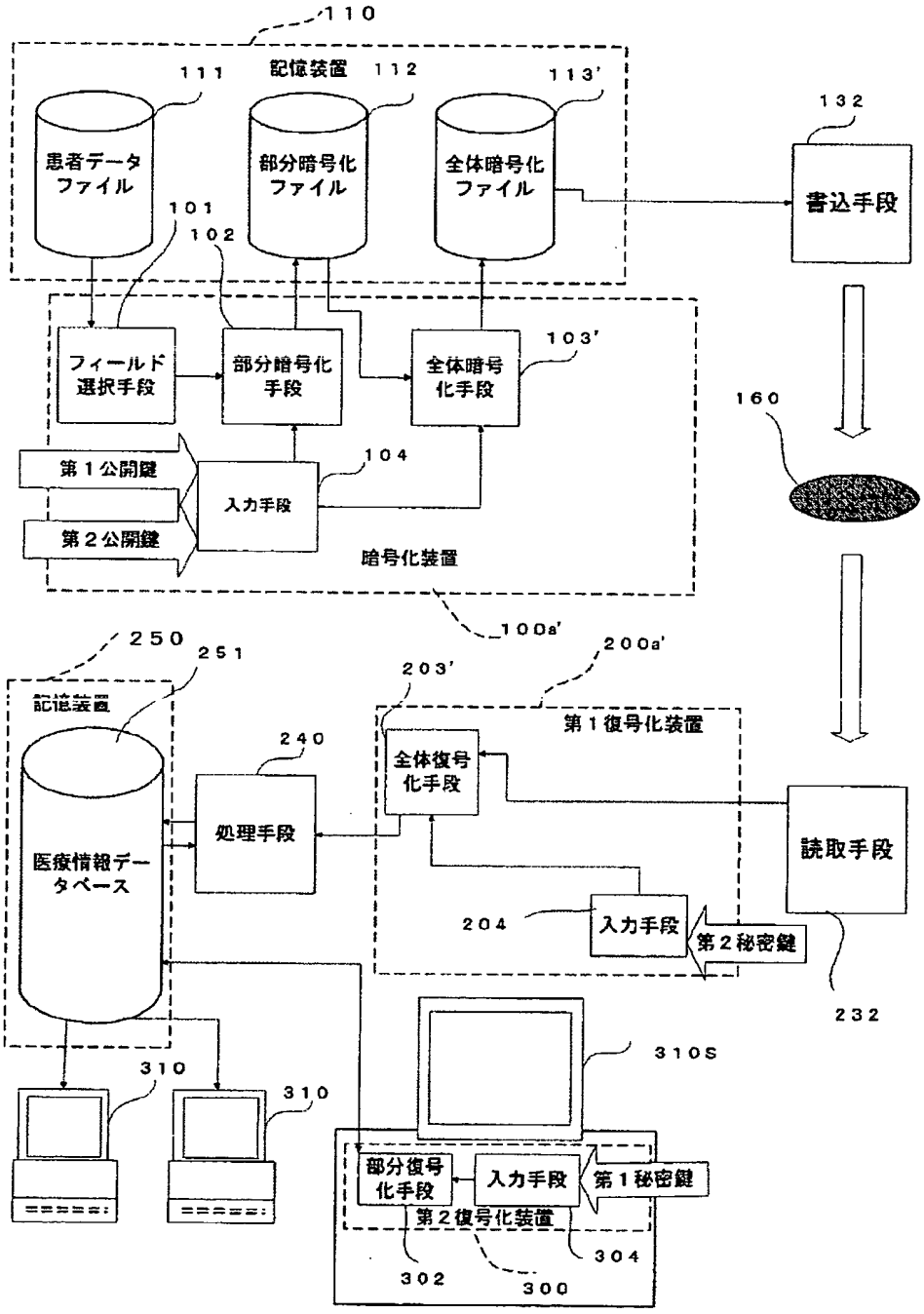
【図7】


110
記憶装置
111
患者データファイル
112
部分暗号化ファイル
113
全体暗号化ファイル
131
通信手段
101
102
103
フィールド選択手段
部分暗号化手段
全体暗号化手段
106
共通鍵暗号化手段
第２公開鍵
第１公開鍵
104
入力手段
共通鍵
暗号化装置
150
インターネット
100b
200b
250
251
203
記憶装置
第１復号化装置
240
全体復号化手段
共通鍵
共通鍵復号化手段
処理手段
医療情報データベース
206
204
入力手段
第２秘密鍵
通信手段
231
310S
310
310
部分復号化手段
入力手段
第１秘密鍵
第２復号化装置
304
302
300

【図9】


スタート
S41
受信
S42
第２秘密鍵の取得
S43
共通鍵の復号化
S22
共通鍵の取得
S23
全体復号化
S24
データベースの創成
S25
第１秘密鍵の入力あり？
はい
S26
部分復号化
いいえ
統計処理・解析処理
S27
エンド

【図10】


110
記憶装置
111
患者データファイル
112
部分暗号化ファイル
113'
全体暗号化ファイル
132
書込手段
101
102
フィールド選択手段
部分暗号化手段
全体暗号化手段
103'
160
第１公開鍵
第２公開鍵
入力手段
104
暗号化装置
100a'
200a'
203'
第１復号化装置
250
251
記憶装置
240
全体復号化手段
処理手段
医療情報データベース
読取手段
204
入力手段
第２秘密鍵
232
310S
310
310
部分復号化手段
入力手段
第１秘密鍵
第２復号化装置
302
300
304